Information Systems
Audit and Control
Association
Virginia Chapter

ISACA-VA, in conjunction with **Canaudit, Inc.** and the **Richmond Police Academy**,
is excited to announce the following course selection for our 2005 Spring Seminar!

Computer Forensics

Overview: The need for agencies and businesses to become more efficient and integrated with one another, as well as the home user, has given way to a new type of criminal, the "*cyber-criminal*." It is no longer a matter of "will your organization be comprised (hacked)?" but, rather, "when?" Today's battles between corporations, governments, and countries are no longer fought only in the typical arenas of boardrooms or battlefields using physical force. Now the battlefield starts in the technical realm, which ties into most every facet of modern day life. If you or your organization requires the knowledge or skills to identify, track, and prosecute the cyber-criminal, then this is the course for you.

This course will give participants the necessary skills to identify an intruder's footprints and to properly gather the necessary evidence to prosecute. Many of today's top tools of the forensic trade will be demonstrated during this course, including software, hardware and specialized techniques.

Who Should Attend:

This course is targeted towards auditors, system administrators, Information Technology personnel, security and law enforcement professionals requiring the knowledge and skills to track down and prosecute the perpetrator. There is no prerequisite for this class. It is designed to increase the knowledge of participants of all levels. Seminar topics will include:

- Introduction to Computer Crimes
- Understanding Computer Forensic
- Tracking the Culprit
- Tools of the Trade
- Preserving Evidence
- Evidence Analysis
- Computer Forensics and the Law
- Checklists and Resources

Date & Time: Tuesday and Wednesday, March 22 & 23, 2005
2 days (16 CPEs and or 16 hours in-service training)
8:00 a.m. to 5:00 p.m.,
Sign-in and continental breakfast begin at 7:15 a.m.

Location: **Richmond Police Academy- Virginia Union University**
1202 W. Graham Road, Richmond, VA 23220

Seminar Price: $450 (Regularly $695)
Price includes continental breakfast, lunch and refreshments throughout the day

Registration deadline March 8, 2005

Registration:

Please **e-mail** or **call** Butch Johnstone at butch.johnstone@dcjs.virginia.gov / (804) 786-3979 Richmond or (540) 561-6656 Roanoke to reserve your spot today. Space is limited - Be sure to Register Early!

Payment:

All payments must be received by March 8, 2008 to ensure your spot for the course. Registration forms are available on the web at www.isaca-va.org/. Checks should be made payable to **ISACA** and mailed to the following address:

ISACA – VA
Attn: Butch Johnstone
Dept. of Criminal Justice Services
3743 Round Hill Ave NW
Roanoke, VA 24012

Cancellations and Substitutions:

If you find it necessary to cancel your conference registration, a full refund less an administrative fee of $50 will be issued for cancellations received up to 10 days before the event. The registration fee is non-refundable for cancellations made less than 10 days before the program. You may provide a substitution at any time.

Accommodations:

Hotel information can be provided upon request.

The Commonwealth of Virginia, Department of Criminal Justice Services, awards Law Enforcement In-service Training Hours. Instructions for obtaining the in-service credits will be available at the seminar.

Canaudit, Inc. is registered with the National Association of State Boards of Accountancy (NASBA), as a sponsor of continuing professional education on the National Registry of CPE Sponsors. State boards of accountancy have final authority on the acceptance of individual courses for CPE credit. Complaints regarding registered sponsors may be addressed to the National Registry of CPE Sponsors, 150 Fourth Avenue North, Suite 700, Nashville, TN 37219-2417. NASBA phone number: 615.880.4200 Web site: www.nasba.org

Computer Forensics for Security & Audit Professionals

COURSE DURATION: 2-days
CPE HOURS: 16
LEVEL: Advanced / Group-Live
PREREQUISITES: None

This course will give participants the necessary skills to identify an intruder's footprints and to properly gather the necessary evidence to prosecute. Many of today's top tools of the forensic trade will be demonstrated during this course, including software, hardware and specialized techniques.

The need for businesses to become more efficient and integrated with one another, as well as the home user, has given way to a new type of criminal, the "*cyber-criminal*." It is no longer a matter of "will your organization be comprised (hacked)?" but, rather, "when?" Today's battles between corporations, governments, and countries are no longer fought only in the typical arenas of boardrooms or battlefields using physical force. Now the battlefield starts in the technical realm, which ties into most every facet of modern day life. If you or your organization requires the knowledge or skills to identify, track, and prosecute the cyber-criminal, then this is the course for you.

WHO SHOULD ATTEND

This course is targeted towards auditors, system administrators, Information Technology personnel, and all other security professionals requiring the knowledge and skills to track down and prosecute the perpetrator. There is no prerequisite for this class. It is designed to increase the knowledge of participants of all levels.

SEMINAR OUTLINE

I INTRODUCTION
- Computer Crime in the news

II UNDERSTANDING COMPUTER FORENSICS
- What is computer forensics?
- Terminology
- How it applies to you
- Information Warfare
- Hackers, Crackers & Cyberterrorists
- Networking basics
  - Communications
  - Devices
- Identifying your vulnerabilities

III TRACKING THE CULPRIT
- Need for thorough documentation
- What do you have to work with?
  - Written Policies
  - Technical Policies
  - Permissions
  - Billing statements
- System, application, & device logs
- Monitoring suspects
  - Employer rights
  - Employee rights
  - Internet tracking
  - Email tracking
- Identifying a culprits tracks and signature
- Creating a profile

IV TOOLS OF THE TRADE
- Software monitoring tools
  - O/S first
  - Key loggers
  - System trackers
- Software recovery tools
  - Data Integrity
  - Recovery/search
  - Data wiping
- Software imaging tools
- Hardware monitoring tools
  - Cameras
  - Key loggers
  - Recording devices
- Password crackers
- Sniffers
- Encryption
- Intrusion detection tools

V PRESERVING EVIDENCE
- Securing the crime scene
- Backing up original data
  - Disk imaging
- Securing your data
  - Public/Private Key
  - Tokens
  - Permissions
  - Seals
- Validation / Authentication
  - Kerberos
  - Digital Certificates
  - Biometrics

VI EVIDENCE ANALYSIS
- The many forms of digital evidence
- General guidelines for analyzing evidence
- What to look for
- Data classification
- Data reconstruction
- Need for cooperation of agencies & departments

VII COMPUTER FORENSICS AND THE LAW
- Investigative procedures
  - Required search & seizure procedures
  - Your company's ethics
- Reconstructing the crime
- Computer fraud & abuse act
- Electronic communications & privacy act
- Case studies & cybercrimes
- Presentation of evidence

VIII CHECKLISTS & RESOURCES
- Computer forensic checklists & resources
- Computer forensic resources

Chris Schroeder

(Home Base: Simi Valley, California)

Chris Schroeder

Chris Schroeder, CISM is Senior Manager, Technical Audit & Security Services with Canaudit and a team leader of the Canaudit Penetration Team and Lightning Strike Force. He is internationally recognized as an expert in the Windows NT and 2000 environments. Chris is a published author on many security-related topics, including network security. He has an impressive track record in his chosen specialties of network penetration and vulnerability assessment, operating systems audits, network audits, and forensic investigations. Since joining Canaudit, Chris has developed new audit and security techniques that have enabled Canaudit to become one of the preeminent audit consulting and security firms in the United States. His pioneering work in wireless LAN security has set the standard for others to follow.

As a former United States Marine, Chris has a unique insight when performing physical security audits. In fact, Chris, along with Canaudit's President - Gordon Smith, has written a physical security guide which is available at the Canaudit website www.canaudit.com. In addition to physical security, Chris has performed many forensic audits and has been studying the legalities of the Patriot Act.

As an experienced seminar leader and conference speaker, Chris draws on his vast experience with network security, penetration audits, and electronic commerce to easily translate complex technical issues into language readily understood by participants at all levels. Because of his experience in web designing and extranet security consulting, Chris skillfully assists Canaudit clients with e-commerce applications and implementation of e-business solutions.

Chris is not only a highly proficient instructor, but he has also developed several Canaudit courses. His latest contribution, *Control and Security of Web Applications* is one of Canaudit's most popular courses.

Chris enjoys the security field, particularly the rapidly changing environment and the challenges it poses. He is constantly adapting and testing new security exploits in his efforts to further the audit and security professional body of knowledge.